Security Advisory 2024-088

Chrome ZeroDay Vulnerabilities

2024-08-27 — v1.1

TLP:CLEAR

History:

- *23/08/2024 — v1.0 – Initial publication*
- *27/08/2024 — v1.1 – Added information about another vulnerability*

Summary

A critical zero-day vulnerability, CVE-2024-7971, has been identified and patched in Google Chrome. This marks the ninth such vulnerability discovered in 2024. The flaw, which has been actively exploited in the wild, is rooted in a type confusion issue within Chrome's V8 JavaScript engine. This vulnerability allows attackers to potentially execute arbitrary code on affected systems [1].

[New] On August 26, Google announced that it patched the tenth zero-day vulnerability in Chrome. This vulnerability is also reported as being exploited [1].

Technical Details

[Updated] The vulnerability **CVE-2024-7971**, with a CVSS score of 8.8, is a type confusion vulnerability in the V8 JavaScript engine used by Google Chrome. Type confusion errors occur when a resource, such as a pointer or object, is allocated as one type but later accessed using a different, incompatible type. This discrepancy can lead to logical errors, including memory corruption, which attackers can exploit to execute arbitrary code or cause the browser to crash. The vulnerability was discovered by the Microsoft Threat Intelligence Center and the Microsoft Security Response Center, and Google has confirmed its exploitation in the wild.

[New] The vulnerability **CVE-2024-7965**, with a CVSS score of 8.8, is due to improper security checks that lead to heap corruption. An attacker can exploit this vulnerability via specifically crafted HTML pages.

Affected Products

- Google Chrome versions prior to 128.0.6613.84/.85 on Windows and macOS.
- Google Chrome versions prior to 128.0.6613.84 on Linux.

Recommendations

Users and administrators should update to the latest stable version (128.0.6613.84/.85) on all platforms.

References

[1] https://chromereleases.googleblog.com/2024/08/stable-channel-update-for-desktop_21.html